Amendments to the Specification

Please amend the specification as follows:

Amend the subparagraph on page 2 beginning on line 11 as follows:

- Coding data ~~on the part of~~ at the sender with at least an individual sender identification,

Amend the subparagraph on page 2 beginning on line 13 as follows:

- Decoding data ~~on the part of~~ at the recipient and checking the individual sender identification and validity,

Amend the last subparagraph on page 2 beginning on line 17 as follows:

- Allocation of user rights for status alteration of transferred data and/or of the control apparatus in accordance with an authorization list filed ~~on the part of~~ at the recipient to the extent that the individual sender identification is entered in the authorization list,

Amend the second full paragraph on page 3 as follows:

A preferred embodiment provides that the data ~~are~~ is coded ~~on the part of~~ at the sender with a digital signature and/or a public key and that the data ~~are~~ is decoded ~~on the part of~~ at the recipient with an associated secret key and/or the digital signature is verified. This means that each transfer of data to or from a control apparatus as a memory-

programmable control unit (SPS) is digitally signed (digital signature). Following a transfer, the signature is first checked, If this is valid, the transferred data ~~are~~ is rejected. Otherwise, it is verified whether the signer has the necessary rights to conduct the transfer. To the extent that the sender possesses the rights, the data ~~are~~ is processed. Otherwise, the transferred data ~~are~~ is rejected.

On page 4, amend the paragraph beginning on line 1 as follows:

If a user digitally signs data, he adds his digital signature and if need be his certificate to the data. A certificate consists, as typical in the area of digital signatures, at least of the identification and the public key of the certificate holder and the digital signature of the certificate issuer on the holder data. The digital signal can be used in the control apparatus for verification of identity and authorization of the sender or signer and the associated public key in order to answer with coded data which only the original sender can read with his private key. There also exists the possibility of coding the data ~~on the part of~~ of the sender with the public key of a recipient and its control apparatus.

Amend the paragraph beginning on line 4 of page 5, as follows:

Preferably the authorization list is deposited into a memory of the control apparatus ~~on the part of~~ of the recipient. The memory range itself can be selectively actuated through the coding of the data to be transferred. The authorization list is also individually adaptable.

Amend the paragraph beginning on line 6 of page 6, as follows:

The memory range of the control apparatus is subdivided into definable regions whereby for each memory range, rights are definable in an authorization list for various sender identifications. For example the manufacturer can grant rights such that a firmware memory range can only be manipulated by a sender identification allocated to the manufacturer. In this way, there results the advantage that firmware, for example through ~~the~~ an Intranet, can be updated or can be delivered in the form of a data set which a client of the memory-programmable control unit stores in this himself/herself. Since the signature of the data loses its validity in the event of a manipulation, only the authorized update can be imported.

Amend the paragraph beginning on line 3 of page 8, as follows:

The data set 10 to be sent is first of all coded in that a digital signature 18 of user 12 and a public key ~~(~~20~~)~~ are added to the data set 10. The combination on the basis of digital signature 18 and public key 20 can also be designated as a certificate which is obtainable at certification authorities (CA) such as Veri Sign for example. The data set 10' signed or coded in this way is transmitted coded over medium 14. In the memory-programmable control unit 16, a root certificate 22 is contained, including a digital signature 24 as well as a secret private and/or public key ~~20~~ 26 in order to decode data set 10'. If the signature 18 is invalid, the transferred data set 10' is rejected. If the signature 18 is valid, then it is verified whether the user 12 has the necessary rights to conduct the transfer. For this, an authorization list 28 is filed in the control apparatus 16 in the form of a table. If these rights exist, the data set 10 can be processed. A memory range of the memory-programmable control unit 16 is subdivided into definable areas (BSS, PS, DS) in accordance with the embodiment. For each memory area, as for example, operating system memory (BSS), program memory (PS) as well as data memory (DS), rights, such as, for example, read (L) and/or write (S) are defined in table 28 for each sender identification ID1...IDn, that is for each sender-side digital signature ID 1, ID 2...IDn.